UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,517	12/11/2003	Gernot Eckstein	I0046.0162	1592

38881 7590 05/27/2011
DICKSTEIN SHAPIRO LLP
1633 Broadway
NEW YORK, NY 10019

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2436	
MAIL DATE	DELIVERY MODE
05/27/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/735,517	**Applicant(s)** ECKSTEIN ET AL.	
	Examiner CARLTON JOHNSON	**Art Unit** 2436	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 12 May 2011 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☒ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1,3 and 5-10*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. ☐ Other: _____.

/Nasser Moazzami/
Supervisory Patent Examiner, Art Unit 2436

/Carlton V. Johnson/
Examiner, Art Unit 2436

Examiner Position:

The arguments were not persuasive in overcoming the currently rejected claims.

Response to Remarks

1. Applicant argues on page 2 of Remarks that power is not the same as voltage. The Examiner disagrees, in Kocher the term power is used to indicate an entity (some form of energy) that is used to make the circuit perform its indicated functions. In the claimed invention, voltage is used to make the claimed circuit perform its indicated functions. In this particular situation, the terms power and voltage respectively for Kocher and the claimed invention are equivalent or analogous terms performing equivalent functions. Kocher discloses varying power which is equivalent to the claimed voltage to time shift operations of the indicated circuit.

2. Applicant argues that Kocher does not disclose time shifting operations within an asynchronous circuit. The Examiner disagrees since the overall claimed entity is a circuit. Within this particular circuit, a source of energy is varied based on time in order to time shift the operations of the circuit.

Kocher discloses that D/A output is provided to a noise production module and that the noise production module is configured to sink power or vary power which also varies the supply voltage. Kocher also discloses that a noise production module may be clocked independently or made to appear to be time-shifted in reference to the execution of other processes. (see Kocher col 5, lines 24-26: D/A output provided to noise production module, which is configured to sink power; col 5, lines 44-47: prevent noise (used to sink or vary power) from being correlated with externally measurable events (operation of processes); multiple noise production modules utilized; col 5, lines 50-60: noise production modules may include delay lines that temporarily isolate their outputs from those of others or they may be clocked independently)

Kocher discloses sinking or varying power (supply voltage) and Kocher also discloses time-shifting the execution of operations. Both events (varying power and time-shifting operation) are produced in correlation to the noise production module.

3. Applicant argues on pages 2 and 4 that Kocher does not disclose time varying a supply voltage of an asynchronous circuit using a random number generator.

The Examiner disagrees. The indicated UART is disclosed in the section discussing clock skipping. The sections discussing random noise generation and clock skipping indicate different procedures to complete random noise generation and clock skipping. The section on clock skipping also discusses clock skipping in relation to random noise generation (see Kocher col 7, lines 19-34). Kocher also discloses in Figure 2 (200, 205) that output from the random number generator is input to the clock skipping module. Kocher discuses the random number generator and clock skipping within the same particular section. Different alternatives to implement random number generation and clock skipping are presented. Theses processes (clock skipping and random number generator) indicated within Kocher are not mutually exclusive alternatives.

The UART is disclosed in reference to the implementation of clock skipping with two clocks (an external clock and an internal clock). The UART is used as a buffer between the internal clock region and the I/O interface to ensure it is clocked at the external clock rate. Kocher discloses the implementation of two separate clock signals (external clock and internal clock). Kocher also discloses that this implementation (2 clocks) makes it more difficult for an attacker to locate points of interest if noise is introduced into signal using techniques of present invention. Noise is introduced into the signal using a random number generator. Noise from a random number generator is used to time shift a clock signal. (see Kocher col 7, lines 6-15) the creation of a separate internal clock signal used to control processor timing during cryptographic operation; noise is also introduced into the signal using the techniques of the present invention)

4. Applicant argues, time varying a supply voltage of an asynchronous circuit using a random number generator.

The indicated UART is disclosed in the section discussing clock skipping. The sections discussing random noise generation and clock skipping indicate different procedures to complete random noise generation and clock skipping. The section on clock skipping also discusses clock skipping in relation to random noise generation (see Kocher col 7, lines 19-34). Kocher also discloses in Figure 2 (200, 205) that output from the random number generator is input to the clock skipping module. Kocher discuses the random number generator and clock skipping within the same particular section. Different alternatives to implement random number generation and clock skipping are presented. Theses processes (clock skipping and random number generator) indicated within Kocher are not mutually exclusive alternatives.

The UART is disclosed in reference to the implementation of clock skipping with two clocks (an external clock and an internal clock). The UART is used as a buffer between the internal clock region and the I/O interface to ensure it is clocked at the external clock rate. Kocher discloses the implementation of two separate clock signals (external clock and internal clock). Kocher also discloses that this implementation (2 clocks) makes it more difficult for an attacker to locate points of interest if noise is introduced into signal using techniques of present invention. Noise is introduced into the signal using a random number generator. Noise from a random number generator is used to time shift a clock signal. (see Kocher col 7, lines 6-15) the creation of a separate internal clock signal used to control processor timing during cryptographic operation; noise is also introduced into the signal using the techniques of the present invention)

5. In conclusion, the circuit of Kocher is an asynchronous type circuit. Kocher discloses time varying a supply voltage. Kocher discloses that D/A output is provided to a noise production module which is configured to sink power or vary power (supply voltage). And, Kocher discloses that a noise production module may be clocked independently or made to appear to be time-shifted. (see Kocher col 5, lines 50-60: to drive noise production module faster than or independently from clock rate applied to cryptosystem microprocessor (time shift operations) The noise production module utilizes a random number generator and is configured to sink power or vary power and time shifts operations. (Kocher col 9, lines 3-9: asynchronous receiver/transmitter; col 5, lines 24-26: D/A output provided to noise production module; configured to sink power; col 5, lines 44-56: prevent noise (sink power) from being correlated to clock transitions (time shifting operations))